

CONTINUED FRACTIONS IN 2-STAGE EUCLIDEAN QUADRATIC FIELDS

XAVIER GUITART AND MARC MASDEU

ABSTRACT. We discuss continued fractions on real quadratic number fields of class number 1. If the field has the property of being 2-stage euclidean, a generalization of the euclidean algorithm can be used to compute these continued fractions. Although it is conjectured that all real quadratic fields of class number 1 are 2-stage euclidean, this property has been proven for only a few of them. The main result of this paper is an algorithm that, given a real quadratic field of class number 1, verifies this conjecture, and produces as byproduct enough data to efficiently compute continued fraction expansions. If the field was not 2-stage euclidean, then the algorithm would not terminate. As an application, we enlarge the list of known 2-stage euclidean fields, by proving that all real quadratic fields of class number 1 and discriminant less than 8000 are 2-stage euclidean.

1. INTRODUCTION

Let F be a number field with maximal order \mathcal{O}_F . Given a list of elements $q_1, \dots, q_n \in \mathcal{O}_F$ the (finite) *continued fraction* $[q_1, \dots, q_n]$ is the element of F defined inductively by:

$$[q_1] = q_1, \quad [q_1, q_2] = q_1 + \frac{1}{q_2}, \quad \dots, \quad [q_1, q_2, \dots, q_n] = [q_1, [q_2, \dots, q_n]].$$

In the case $F = \mathbb{Q}$, it is a classical result that every $x \in \mathbb{Q}$ is a continued fraction with coefficients in \mathbb{Z} , which can be effectively computed by means of the euclidean algorithm. This property is no longer true for arbitrary F . Indeed, one has the following result (cf. [1] Theorem 1, Corollary 3 and Proposition 13).

Theorem 1.1 (Cooke-Vaseršteĭn). *Suppose that \mathcal{O}_F^\times is infinite. Then every element in F is a continued fraction with coefficients in \mathcal{O}_F if and only if F has class number 1.*

Unlike in the classical case, the proof of this theorem is not constructive. Indeed, the ring \mathcal{O}_F is not euclidean in general, which makes it hard to effectively compute continued fractions of elements in F . There is a huge amount of literature devoted to euclidean rings, a number of generalizations and their relation with continued fractions algorithms, mainly motivated by their applications to the arithmetic of number fields. A survey of these topics can be found in [11].

Continued fractions in number fields also arise in the computation of Hecke eigenvalues of automorphic forms, via the modular symbols algorithm. See for instance [4] for the case of imaginary quadratic fields, or [8] for an account in

Date: January 27, 2013.

2010 *Mathematics Subject Classification.* Primary 13F07, 11A55.

Partially supported by Grants MTM2009-13060-C02-01 and 2009 SGR 1220.

the setting of Hilbert modular forms. As a more recent application, we mention that the computation of continued fractions turns out to be a critical step in the effective computation of ATR points in elliptic curves over real quadratic fields of class number 1. ATR points are Stark-Heegner points defined over Almost Totally Real fields. See [5, §4] for a discussion of the role played by continued fractions in this kind of computations, and [7, Example 6] for another example of their use.

In this note we restrict ourselves to the case of F being a real quadratic number field of class number 1. We build on the approach taken by Cooke in [1], and we provide an algorithm that (under an appropriate version of the Generalized Riemann Hypothesis) computes a continued fraction of any element $x \in F$. To be more precise, we circumvent the problem that most of these fields are not euclidean by exploiting the property of being 2-stage euclidean.

A *1-stage division chain* for a pair of elements $\alpha, \beta \in \mathcal{O}_F$ is a pair (q_1, r_1) of elements in \mathcal{O}_F satisfying $\alpha = q_1\beta + r_1$. A *2-stage division chain* is a quadruple (q_1, q_2, r_1, r_2) of elements in \mathcal{O}_F satisfying:

$$\begin{aligned}\alpha &= q_1\beta + r_1 \\ \beta &= q_2r_1 + r_2.\end{aligned}$$

A field F is said to be *2-stage euclidean* (with respect to the norm Nm of F/\mathbb{Q}) if any pair of elements $\alpha, \beta \in \mathcal{O}_F$, with $\beta \neq 0$, has a *k-stage decreasing chain* for $k \leq 2$; that is, a *k-stage division chain* as above satisfying the additional property

$$|\text{Nm}(r_k)| < |\text{Nm}(\beta)|.$$

In general, the notion of *n-stage euclidean* is defined by means of division chains of length at most n , but it is enough for our purposes to restrict to $n = 2$.

Given a 2-stage euclidean field F , (in fact, any *k-stage euclidean* field), a variation of the usual proof of the fact that euclidean implies class number 1 shows that F is of class number 1. Conversely, it is expected that all real quadratic fields of class number 1 are 2-stage euclidean. Indeed, in [3] it is proven that if certain Generalized Riemann Hypothesis holds then every real quadratic field of class number 1 is 2-stage euclidean. In spite of this result, up to now only a few real quadratic fields have been proven to be 2-stage euclidean: as reported in [11, p. 14], they are the fields $\mathbb{Q}(\sqrt{m})$ with m belonging to the set

$$(1.1) \quad \{ \mathbf{2}, \mathbf{3}, \mathbf{5}, \mathbf{6}, \mathbf{7}, \mathbf{11}, \mathbf{13}, 14, \mathbf{17}, \mathbf{19}, \mathbf{21}, 22, 23, \mathbf{29}, 31, \mathbf{33}, \mathbf{37}, 38, \mathbf{41}, 43, \\ 46, 47, 53, \mathbf{57}, 59, 61, 62, 67, 69, 71, \mathbf{73}, 77, 89, 93, 97, 101, 109, 113, 129, \\ 133, 137, 149, 157, 161, 173, 177, 181, 193, 197, 201, 213, 253 \},$$

where those numbers appearing in bold face correspond to the complete list of norm-euclidean rings. The purpose of this note is to present an algorithm for checking 2-stage euclideanity of real quadratic fields, thus allowing the computation of continued fractions. The main result of the article is the following theorem.

Main Theorem 1. *There exists an algorithm that:*

- (i) *accepts as input a real quadratic field F ; if F is 2-stage euclidean the algorithm terminates and it proves that F is 2-stage euclidean.*
- (ii) *if F is 2-stage euclidean, after finishing step (i) it accepts as input any $x \in F$ and it computes a continued fraction with coefficients in \mathcal{O}_F for x .*

Remark 1.2. If the field F is not 2-stage euclidean then the algorithm will not terminate. However, in an actual implementation the algorithm would either run

out of memory or break due to rounding errors. However, as expected, we haven't been able to observe this phenomenon because all tested fields are indeed 2-stage euclidean.

As will be explained in more detail in the subsequent sections, for a given field F what step (i) does is a precomputation of the data that is needed in order to compute a 2-stage decreasing chain for any $\alpha, \beta \in \mathcal{O}_F$ with $\beta \neq 0$. If F is 2-stage euclidean the algorithm succeeds in this precomputation, which at the same time constitutes a proof that F is 2-stage euclidean. Then the data generated in (i) is used in (ii) to compute the continued fraction of any $x \in F$.

An implementation of the algorithm has been submitted as a patch to Sage, and it is available at http://trac.sagemath.org/sage_trac/ticket/11380. As an application, we have extended list (1.1) by proving that all real quadratic fields of class number 1 and discriminant up to 8000 are 2-stage euclidean.

The plan of the paper is as follows: In Section 2 we recall the basic notions of 2-stage euclidean fields and their relation with the computation of continued fractions. In Section 3 we describe and prove the correctness of the algorithm in Main Theorem 1. In Section 4 we comment on some implementation details and we also include some data arising from numerical experiments. As we will see, they suggest a measure of euclideanity for quadratic fields that, to the best of our knowledge, have not been considered before.

It is a pleasure to thank Jordi Quer for his comments on an earlier version of the manuscript. We are also grateful to the referee for valuable observations and suggestions.

2. CONTINUED FRACTIONS AND 2-STAGE EUCLIDEAN FIELDS

We begin this section by recalling the basic definitions and properties that we will use. Let m be a positive squarefree integer and let $F = \mathbb{Q}(\sqrt{m})$. Let $\omega = (1 + \sqrt{m})/2$ if $m \equiv 1 \pmod{4}$ and $\omega = \sqrt{m}$ if $m \equiv 2, 3 \pmod{4}$, so that the ring of integers is $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\omega$. Let α/β be an element of F . If F is 2-stage euclidean one can find a k -stage decreasing chain for the pair α, β with $k \leq 2$. If the last residue r_k is not zero, one can then repeat this process to end with a division chain

$$\begin{aligned} \alpha &= q_1\beta + r_1 \\ \beta &= q_2r_1 + r_2, \\ r_1 &= q_3r_2 + r_3 \\ r_2 &= q_4r_3 + r_4 \\ &\vdots \\ r_{n-2} &= q_nr_{n-1} + r_n \end{aligned}$$

with $r_n = 0$, because the norm of the corresponding residue decreases in absolute value at worst every two steps. The classical formulas for the case of rational numbers (cf. [10, §10.6]) show that α/β is then equal to the continued fraction $[q_1, \dots, q_n]$. Therefore, part (ii) of Main Theorem 1 is straightforward if one can compute 2-stage decreasing chains for arbitrary pairs of elements in \mathcal{O}_F . We remark, however, that α/β may admit many different representations as a continued fraction, since 2-stage decreasing chains are not unique.

The following is a particular case of [1, Corollary 1].

Proposition 2.1. *There exists a 2-stage decreasing chain for α, β if and only if there exists a continued fraction of length 2, say $[q_1, q_2]$, such that*

$$\left| \text{Nm} \left(\frac{\alpha}{\beta} - [q_1, q_2] \right) \right| < \frac{1}{|\text{Nm}(q_2)|}.$$

Let v_1, v_2 denote the two embeddings of F into \mathbb{R} , and let $v = (v_1, v_2): F \hookrightarrow \mathbb{R}^2$. Concretely, it is given by $1 \mapsto (1, 1)$ and $\sqrt{m} \mapsto (\sqrt{m}, -\sqrt{m})$. We will often identify F with $v(F)$, even without explicitly mentioning v . The norm of F extends to \mathbb{R}^2 via the formula

$$\text{Nm}(x, y) = xy, \quad \text{for } x, y \in \mathbb{R}.$$

Let CF_2 denote the set of continued fractions of length at most 2. Any element in \mathcal{O}_F can be expressed as a continued fraction of length 2, so CF_2 is also the set of continued fractions of length exactly 2. For a positive integer n , let

$$\text{CF}_2(n) = \{q = [q_1, q_2] \in \text{CF}_2 : |\text{Nm}(q_2)| \leq n\}.$$

For $q = [q_1, q_2] \in \text{CF}_2$ define

$$V(q) = \left\{ x \in \mathbb{R}^2 : |\text{Nm}(x - q)| < \frac{1}{|\text{Nm}(q_2)|} \right\}.$$

In the subsequent sections it will be useful to refer to q_2 as the *denominator* of $V(q)$. The region $V(q)$ is bounded by the hyperbolas

$$(x - x_0)(y - y_0) = \frac{\pm 1}{|\text{Nm}(q_2)|},$$

where $(x_0, y_0) = v(q)$. From Proposition 2.1 we see that F is 2-stage euclidean if and only if \mathbb{R}^2 can be covered by open sets of the form $V(q)$, with $q \in \text{CF}_2$. The knowledge of such a covering also translates into a method for computing a 2-stage decreasing chain for a pair α, β : if α/β belongs to $V([q_1, q_2])$, then q_1 and q_2 are the quotients of such a chain.

Let γ be an element in \mathcal{O}_F . Then x belongs to $V([q_1, q_2])$ if and only if $(x - \gamma)$ belongs to $V([q_1 - \gamma, q_2])$. So instead of $x \in F$ one can work with \bar{x} , its class modulo \mathcal{O}_F , which as an element of \mathbb{R}^2 lies in the fundamental domain

$$D = \{av(1) + bv(w) : a, b \in [0, 1)\}.$$

The advantage is that \overline{D} is compact, so finite coverings are enough.

Proposition 2.2. *The quadratic field F is 2-stage euclidean if and only if D can be covered by finitely many hyperbolic regions $V(q)$ with q belonging to CF_2 .*

From Proposition 2.2 we can already see the idea of an algorithm for checking whether F is 2-stage euclidean. It is easy to define an ordering on the set of continued fractions $q = [q_1, q_2] \in \text{CF}_2$. One can then generate such q 's in order, and check at each step whether the sets $V(q)$ for the q generated so far already cover D . If F is 2-stage euclidean this process will necessarily finish, producing a finite list of $V(q)$'s that cover D . One can then compute a 2-stage decreasing chain for a pair α, β by finding a $V(q)$ that contains α/β .

However, working with all the sets $V(q)$ for $q \in \text{CF}_2$ is readily seen to be computationally unfeasible. Therefore, one wants to work only with a few of the possible centers, but in a way that the algorithm is still guaranteed to finish. This is essentially what our algorithm does. At this point we remark that the algorithm presents two critical points:

- (1) How to choose the centers q for the regions $V(q)$ to be considered.
- (2) How to check, algorithmically, whether a collection of sets $V(q)$ covers D .

The next section is devoted to discuss in detail the algorithm and the implementation of these two steps.

3. THE ALGORITHM

In this section we address the two main points raised at the end of the previous section. The centers that will be considered come from the observation that, for each positive integer N , there are finitely many elements $q = [q_1, q_2]$ inside the fundamental domain D with $|\text{Nm}(q_2)| \leq N$. We will take small translates of these centers by elements of \mathcal{O}_F , which moves them outside D , but as long as the corresponding regions still intersect D . The following definitions and results make this more precise.

Given a positive integer N , denote by Q_N the set consisting of continued fractions $q = [q_1, q_2]$ of length two with $|\text{Nm}(q_2)| \leq N$ and such that q belongs to D :

$$Q_N = \{q = [q_1, q_2] : |\text{Nm}(q_2)| \leq N \text{ and } q \in D\}.$$

For a positive integer T , we also define the following set of translates of elements in Q_N :

$$Q_{T,N} = \{q = a + b\omega \in Q_N + \mathcal{O}_F : |b| < T \text{ and } V(q) \cap D \neq \emptyset\}.$$

Proposition 3.1. *The sets Q_N and $Q_{T,N}$ are finite and effectively computable.*

Proof. First we consider the set Q_N . There is a finite number of ideals of norm bounded by N , and there are algorithms to compute them. Since \mathcal{O}_F is a principal ideal domain, the set of ideals of norm up to N is of the form

$$\{(\alpha_1), \dots, (\alpha_k)\},$$

for some (non-canonical) choice of representatives α_i . If β is any element of norm less than or equal to N , it must be of the form $\beta = u\alpha_i$ for some i and some unit u . Therefore:

$$\frac{1}{\beta} = \frac{1}{u\alpha_i} = \frac{u^{-1}}{\alpha_i} \in \frac{1}{\alpha_i}\mathcal{O}_F.$$

Since we are looking for representatives modulo the action of the additive group \mathcal{O}_F , all elements of Q_N are to be found in

$$\bigcup_{i=1}^k \left(\mathcal{O}_F + \frac{1}{\alpha_i}\mathcal{O}_F \right) / \mathcal{O}_F \simeq \bigcup_{i=1}^k \mathcal{O}_F / \alpha_i \mathcal{O}_F,$$

which is finite and computable.

Given positive integers T and N , and an element $q = [q_1, q_2] \in Q_N$, define the set $Q_{q,T,N}$ as:

$$Q_{q,T,N} = \{a + b\omega \in q + \mathcal{O}_F : |b| < T, V(a + b\omega) \cap D \neq \emptyset\}.$$

To prove the finiteness of $Q_{T,N}$ it is enough to show that the sets $Q_{q,T,N}$ are finite for each $q \in Q_N$. Write $q = r + s\omega$ for some $r, s \in \mathbb{Q}$. If q' is an element of $Q_{q,T,N}$, one can write $q' = r + d + (s + t)\omega$ where d and t belong to \mathbb{Z} . Since the absolute value of $s + t$ needs to be bounded by T and s is fixed, there is a finite number of possible choices for t . It remains to show that for each value of t there are finitely many possibilities for d . Let $v(r + (s + t)\omega) = (x_0, y_0)$. Then

$v(q') = v(r + d + (s + t)\omega) = (x_0 + d, y_0 + d)$. The hyperbolic region $V(q')$ is contained in the union of two strips in \mathbb{R}^2 :

$$V(q') \subset R_d^x \cup R_d^y,$$

where

$$R_d^x = \{(x, y) \in \mathbb{R}^2 : |(x - x_0 - d)| < |\text{Nm}(q_2)|^{-1/2}\},$$

$$R_d^y = \{(x, y) \in \mathbb{R}^2 : |(y - y_0 - d)| < |\text{Nm}(q_2)|^{-1/2}\},$$

Since x_0 and y_0 are fixed, it is clear that $R_d^x \cup R_d^y$ intersects D for finitely many values of d . \square

The following lemma allows us to prove that a certain region of \mathbb{R}^2 is covered by hyperbolic regions by doing a finite amount of computation. Its proof is elementary and follows easily from the shape of the regions $V(q)$.

Lemma 3.2. *Let R be a box in \mathbb{R}^2 of the form:*

$$R = R(x_0, x_1, y_0, y_1) = \{(x, y) \in \mathbb{R}^2 : x_0 \leq x \leq x_1 \text{ and } y_0 \leq y \leq y_1\}.$$

Then R is contained in $V(q)$ if each of its four corners is.

Proof. Doing a translation in \mathbb{R}^2 we may and do assume that $V(q)$ is of the form:

$$V(q) = \{(x, y) \in \mathbb{R}^2 : |xy| < \epsilon\},$$

for some positive ϵ . If the four corners of R are contained in $V(q)$, then:

$$|x_i y_j| < \epsilon, \quad i, j \in \{0, 1\}.$$

Given (x, y) belonging to R , we have that:

$$|x| \leq \max\{|x_0|, |x_1|\},$$

and that

$$|y| \leq \max\{|y_0|, |y_1|\}.$$

Therefore:

$$|xy| = |x||y| \leq \max\{|x_0|, |x_1|\} \max\{|y_0|, |y_1|\} < \epsilon.$$

\square

Let R_0 be a box as in Lemma 3.2 such that R_0 contains the fundamental domain D of F . For each positive integer n , subdivide R_0 into 4^n identical boxes, and let $S(R_0)_n$ be the set of these. The following result plays a crucial role in showing the correctness of the algorithm.

Lemma 3.3. *The field F is 2-stage euclidean if and only if there exists a finite set Z of hyperbolic regions and a positive integer L such that each box in $S(R_0)_L$ is contained in at least one of the regions of Z .*

Proof. First assume that F is 2-stage euclidean. Therefore the box R_0 can be covered by hyperbolic regions $V(q)$. Since these are open and R_0 is compact, there is a finite set of hyperbolic regions Z such that R_0 is covered by regions in Z .

Let $S(R_0) = \cup_{n=1}^{\infty} S(R_0)_n$ and let $U \subset R_0$ be the complement of the set of corners:

$$U = R_0 \setminus \bigcup_{R=R(x_0, x_1, y_0, y_1) \in S(R_0)} \{(x_0, y_0), (x_0, x_1), (x_1, y_0), (x_1, y_1)\}.$$

Note that U is dense in R_0 . For each point x in U , let V_x be a region in Z containing x , and let R_x be an element of $S(R_0)$ which is contained in V_x and such that x belongs to R_x . Let n_x be the least integer such that R_x belongs to $S(R_0)_n$.

The set R_0 is covered by the interiors of the boxes R_x as x varies in R_0 , and therefore we can extract a finite covering, say:

$$R_0 = \bigcup_{i=1}^l R_{x_i}.$$

Set L to be the maximum of the integers n_{x_1}, \dots, n_{x_l} . It is easily verified that the set Z and the integer L satisfy the condition of the lemma.

The converse is obviously true, since the hyperbolic regions belonging to Z already cover R_0 , which contains D . \square

The algorithm performing Part (i) of Main Theorem 1 can easily be described in recursive form. Algorithm 1 is the recursive function **SOLVE**, which accepts as input a box R . Algorithm 2 is the main loop.

Algorithm 1 SOLVE

Input: A box R . Global T, N and a computed $Q_{T,N}$. A global vector Z of regions used so far.

Output: The box R is covered by regions in Z .

if there is $q \in Q_{T,N}$ such that $R \subset V(q)$ **then**

Append q to Z .

else

Increase T and N and re-compute $Q_{T,N}$.

Subdivide R into four equal boxes R_1, R_2, R_3, R_4 .

for $i=1$ **to** 4 **do**

SOLVE(R_i)

end for

end if

return

Algorithm 2 Proves that F is 2-stage euclidean.

Input: F a real quadratic number field.

Output: F is 2-stage euclidean.

Find a box R_0 in \mathbb{R}^2 that contains the fundamental domain D .

$Z \leftarrow []$.

Fix some initial N and T and compute the set $Q_{T,N}$.

SOLVE(R_0)

return Z , a list of regions covering the fundamental domain D .

Theorem 3.4. *Algorithm 2 terminates if and only if F is 2-stage euclidean.*

Proof. Note first that Algorithm 2 terminates if and only if the function call to **SOLVE**(R_0) terminates. Suppose that F is 2-stage euclidean, and let Z and L be as given by Lemma 3.3 applied to the box R_0 . Let T, N be such that

$$Z \subseteq Q_{T,N}.$$

The size of the boxes passed to the **SOLVE** function is divided by four each time that the recursion depth increases. On the other hand, both T and N increase as well with the recursion depth. Therefore, for a sufficiently large recursion depth we will have T and N satisfying the above containment, and at the same time boxes considered will belong to $S(R_0)_{L'}$ for some $L' > L$. Hence the algorithm terminates in finite time.

Conversely, if the algorithm terminates it exhibits a list of regions that covers the fundamental domain. Therefore F must be 2-stage euclidean. \square

4. NUMERICAL EXPERIMENTS AND A MEASURE OF EUCLIDEANITY

As an application of the algorithm we have verified the following result.

Theorem 4.1. *All real quadratic number fields of class number 1 and discriminant less than 8,000 are 2-stage euclidean.*

The computations were performed using Sage in a laptop with processor Intel Core 2 Duo T7300 / 2.0 GHz and 2.0 GB of RAM. The time needed for checking the 2-stage euclideanity of a given number field tends to grow with the discriminant. For instance, for discriminants of size about 100 it takes no more than a few seconds, while for discriminants of size about 8000 it can take up to several hours.

In spite of this, the size of the discriminant is not the only factor that determines the computational cost. For instance, we have observed that discriminants of similar size can lead to very different times of execution, depending on the number of small primes that are inert in the field. Recall that the algorithm terminates when it covers the domain D with sets $V(q)$. These $V(q)$ are bounded by hyperbolas of the type $(x - x_0)(y - y_0) = \pm 1/|\text{Nm}(q_2)|$, where q_2 is the denominator of q . A prime p that is not inert in F leads to hyperbolas of the type $(x - x_0)(y - y_0) = \pm 1/p$. However, if p is inert it leads to hyperbolas of the type $(x - x_0)(y - y_0) = \pm 1/p^2$ instead, which are likely to cover a smaller part of D . As an illustration of this phenomenon, we mention that it took 68 seconds to check the 2-stage euclideanity of $\mathbb{Q}(\sqrt{1273})$, where primes 2, 3, and 5 are not inert, whereas it took 1131 seconds to check $\mathbb{Q}(\sqrt{1253})$, where the only prime less than 20 that is not inert is 7.

The sizes of the hyperbolic regions are also related to another factor that can substantially affect the running time: the maximum norm of the denominators of the regions $V(q)$ that are needed to cover D . In order to analyze this influence, it is useful to make the following definition.

Definition 4.2. Let F be a 2-stage euclidean field with fundamental domain D . We say that F is n -smooth euclidean if

$$D \subseteq \bigcup_{q \in \text{CF}_2(n)} V(q);$$

that is, if D can be covered by using regions of denominator up to n .

Let n be the smallest integer such that F is n -smooth euclidean. The complexity of the algorithm depends on n , because it determines the number of hyperbolic regions with center in D to be computed. Indeed, the number of ideals of norm m is $O(m^\varepsilon)$. By (the proof) of Proposition 3.1, there are at most m centers of hyperbolic regions lying in D for each ideal of norm m , thus giving $O(m^{1+\varepsilon})$ centers in D whose denominator has norm m . Since one has to consider all ideals of norm $m \leq n$, the cardinality of the set Q_n is at most $O(n^{2+\varepsilon})$.

However, the algorithm actually works with translations of elements in Q_n . That is, the centers to be considered lie in $Q_{T,n}$ for some T , which corresponds to the maximum length of translations. Unfortunately, to fully determine the complexity of the algorithm we lack an estimation of T , as well as of the integer L in Lemma 3.3, which gives the number of boxes that are to be checked by the function **SOLVE**. We remark that in the implementation used to prove Theorem 4.1 a value of $T = 5$ was enough to solve for all discriminants.

The value of the smallest n such that F is n -smooth euclidean does not only depend on the size of the discriminant, but also on the splitting behavior of small primes. As an illustration of this fact, Figure 1 plots the maximum norm of the denominators that our implementation used to cover the tested number fields, according to their discriminant.

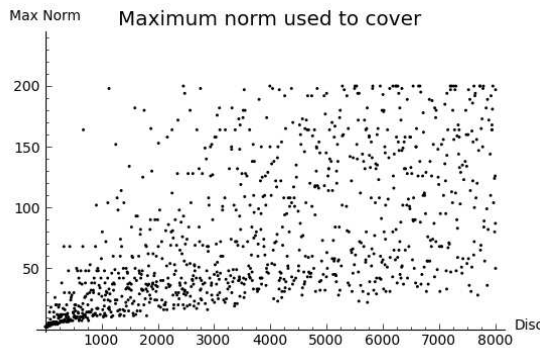


FIGURE 1.

When carrying out this test we initialized the maximum norm to $N = 200$. This explains why the points tend to accumulate towards this value as the discriminant increases. Also notice how, even if the points appear distributed in a random fashion, there is a region on the lower part of the graph where no point lies. This region increases with the discriminant, and in the next subsection we will give an explanation to this phenomenon.

Figure 2 is similar to Figure 1, but only the data for some of the number fields are plotted: those in which both 2 and 3 remain inert are shown as red squares, whereas those in which 2 and 3 split are shown as blue circles.

We remark that if the algorithm manages to cover D using denominators of norm up to n , this implies that F is n -smooth euclidean. However, this does not rule out the possibility that the field could be m -smooth euclidean for some $m < n$. If we knew a priori the smallest n such that F is n -smooth euclidean, we could initialize N in Algorithm 2 to this value and then only increasing T the algorithm would cover D . However, the value of the smallest n is not known a priori, so that the algorithm is not guaranteed to finish if one only increases T . Therefore, the algorithm may have to eventually increase also the maximum norm N , and this can lead to considering norms higher than what is strictly necessary. Actually, the way in which T and N are increased turns out to be the most critical implementation parameter of the algorithm, as for the running time is concerned. In the implementation we used for proving Theorem 4.1 we took a constant value

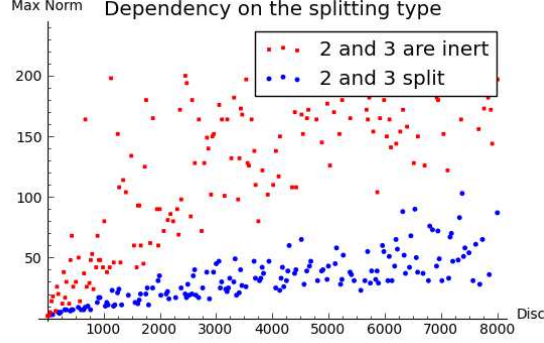


FIGURE 2.

of $T = 5$, and the increasing step for N was proportional to the part of D not being covered (the proportional constant found by fine-tuning).

A measure of euclideanity. Besides its computational influence in our implementation, the smallest n such that F is n -smooth euclidean can also be interpreted as a measure of how far is F from being euclidean. Indeed, it is easily seen that F is n -smooth euclidean if and only if for any pair $\alpha, \beta \in \mathcal{O}_F$, $\beta \neq 0$, one can find $q, r \in \frac{1}{n}\mathcal{O}_F$ such that

$$\alpha = q\beta + r,$$

with $|\text{Nm}(r)| < |\text{Nm}(\beta)|$. In particular, F is 1-smooth euclidean if and only if it is euclidean. In this way, the following statement can be seen as a generalization of the classical result on the existence of finitely many euclidean real quadratic fields.

Theorem 4.3. *Let n be a positive integer. There exist only finitely many n -smooth euclidean real quadratic fields.*

This is a consequence of a well known property of euclidean minima of real quadratic fields. We recall that the *euclidean minimum* of F is defined to be

$$M(F) = \inf\{\mu \in \mathbb{R} : \forall x \in F \exists y \in \mathcal{O}_F \text{ such that } |\text{Nm}(x - y)| \leq \mu\}.$$

Denote by $d(F)$ the discriminant of F . By a result of Ennola [9] we have that for real quadratic fields

$$M(F) \geq \frac{\sqrt{d(F)}}{16 + 6\sqrt{6}}.$$

Theorem 4.3 follows immediately from the following lemma.

Lemma 4.4. *Let n be a positive integer and let $t = \text{lcm}(1, 2, 3, \dots, n)$. If $d(F) > (16 + 6\sqrt{6})^2 \cdot t^4$ then there exists an element $z \in F$ such that*

$$|\text{Nm}(z - q)| > 1 \quad \text{for all } q \in \text{CF}_2(n).$$

Proof. Let z_0 be an element in F with the property that

$$|\text{Nm}(z_0 - \alpha)| \geq \frac{\sqrt{d(F)}}{16 + 6\sqrt{6}} \quad \text{for all } \alpha \in \mathcal{O}_F,$$

and let $z = \frac{z_0}{t}$. Then

$$|\mathrm{Nm}(z - \frac{\alpha}{t})| \geq \frac{\sqrt{d(F)}}{t^2 \cdot (16 + 6\sqrt{6})} > 1 \quad \text{for all } \alpha \in \mathcal{O}_F.$$

This finishes the proof, because $\mathrm{CF}_2(n)$ is contained in $\frac{1}{t}\mathcal{O}_F$. \square

REFERENCES

- [1] G. E. Cooke, *A weakening of the Euclidean property for integral domains and applications to algebraic number theory I*. J. Reine Angew. Math. 282 (1976), 133–156.
- [2] G. E. Cooke, *A weakening of the Euclidean property for integral domains and applications to algebraic number theory. II*. J. Reine Angew. Math. 283/284 (1976), 71–85.
- [3] G. E. Cooke, P. Weinberger, *On the construction of division chains in algebraic number rings, with applications to SL_2* . Comm. Algebra. vol 3 (1975), 481–524.
- [4] J. E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*. Compositio Mathematica, 51 no. 3 (1984), p. 275–324
- [5] H. Darmon and A. Logan, *Periods of Hilbert modular forms and rational points on elliptic curves*. Int. Math. Res. Not. 2003, no. 40, 2153–2180.
- [6] H. Davenport, *Indefinite binary quadratic forms, and Euclid’s algorithm in real quadratic fields*. Proc. London Math. Soc. (2) 53 (1951), 65–82.
- [7] L. Dembélé, *An algorithm for modular elliptic curves over real quadratic fields*. Experiment. Math. 17 (2008), no. 4, 427–438.
- [8] L. Dembélé, J. Voight, *Explicit methods for Hilbert modular forms*. To appear in “Elliptic Curves, Hilbert modular forms and Galois deformations”. [arXiv:1010.5727v2](https://arxiv.org/abs/1010.5727v2).
- [9] V. Ennola, *On the first inhomogeneous minimum of indefinite binary quadratic forms and Euclid’s algorithm in real quadratic fields* Ann. Univ. Turku. Ser. A I 28 (1958), 58pp.
- [10] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*. Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, Oxford, 2008. xxii+621 pp. ISBN: 978-0-19-921986-5, 11-01
- [11] F. Lemmermeyer, *The Euclidean algorithm in algebraic number fields*. Exposition. Math. 13 (1995), no. 5, 385–416.

UNIVERSITAT POLITÈCNICA DE CATALUNYA, BARCELONA
E-mail address: xevi.guitart@gmail.com

COLUMBIA UNIVERSITY, NEW YORK
E-mail address: masdeu@math.columbia.edu